Telecommunications Industry Association
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209 | www.tiaonline.org

June 3, 2025

Noah Jackson
Legislative Clerk
Committee on Energy and Commerce
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Jackson,

The Telecommunications Industry Association ("TIA") appreciates this opportunity to provide additional responses to the Energy and Commerce Subcommittee on Communications and Technology following our testimony during the hearing titled "Global Networks at Risk: Securing the Future of Communications Infrastructure" before the Subcommittee on April 30, 2025. Following the hearing, TIA received Questions for the Record from Ranking Member Doris Matsui, Representative August Pfluger, and Representative Robin Kelly. Attached, please find our responses to those questions.

Thank you again for this opportunity to discuss the importance of trusted and resilient global networks, risks facing the Information Communication Technology sector, and the importance of maintaining a robust and reliable global subsea cable network. We would be happy to answer any follow up questions or meet with any Subcommittee members in the future to discuss these important topics in the future.

David Stehlin
Chief Executive Officer

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard,
Floor 25
Arlington, VA 22209
(703) 907-7700

Attachment —Additional Questions for the Record

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209 | www.tiaonline.org

TIA Responses to Additional Questions for the Record

The Honorable August Pfluger

Last year, I introduced the "Undersea Cable Security and Protection Act" to establish an interagency working group to bolster undersea cables' security, resiliency, and integrity.
It is estimated that 95-99% of the entire world's data travels via subsea cables, and cable cuts have become a common tactic by Russia, China, and Iran's terrorist proxy groups to disrupt communications.

1. ***Mr. Stehlin, please briefly expand upon why protecting subsea cables is important to consumers and the telecommunications industry, as well as why it is within the national security interests of the United States to protect them.***

Response: Subsea cables enable fast, reliable communication for consumers and businesses and supports critical functions key to both the economic and national security of the U.S. The U.S. depends on these cables for efficient data transmission, and any disruption can lead to significant service outages, financial losses, and damage to business operations, particularly for data-heavy industries like finance, cloud computing, and e-commerce.

Subsea cable security is part of broader global infrastructure resilience. Foreign adversaries tampering with these systems could destabilize communications and economic systems, posing serious national security threats. Protecting them ensures the stability of global infrastructure, cross border data flows, and supports both economic and security interests.

I would equate the importance of subsea cable systems to the importance of commercial vessels travelling the seas to carry goods from port to port. As I said in my testimony before the subcommittee, 99% of cross continental internet traffic is carried through these subsea cables. As advanced digital technologies continue to emerge, such as artificial intelligence (AI), xreality (XR), and the Internet of things, subsea cables will continue to become even more essential to the U.S. economy as they connect U.S. innovation to global markets.

I have concerns about the Team Telecom process causing delays in the cable landing deployment process. I worry that these delays in deployment are working against our national and economic security interests. My understanding is the review process has gone from taking 6-9 months under the first Trump Administration to now taking 2-3 years.

2. ***Can you explain the challenges within the Team Telecom review process? Do you believe there is sufficient representation of our economic security interests on Team Telecom?***

Response: The Team Telecom review process suffers chiefly from three challenges: redundancy, transparency, and predictability. A comprehensive subsea cable review begins anew each time a licensee applies, regardless of whether Team Telecom has already reviewed the applying entity. This redundant process often leads our members to submit the same information multiple times. The combination of redundancy and a lack of information sharing between Team Telecom agencies is unfortunately cumulative, requiring the same information to be submitted across multiple applications and then to multiple agencies. The Team Telecom risk assessment process is also opaque, with little economic input, and little insight into how the agencies measure threat, vulnerability and consequence. With little to no consistency over similarly situated projects, and limited regulatory predictability, there is a constant risk of stranded investment for applicants. This results in a process that is harmful for builds that can take decades to result in a return on investment. While the Team Telecom process is important for our national security, the resulting regulatory uncertainty that this process is creating may hamper innovation in a way that results in more harm than good

as we begin to cede our subsea cable leadership to China.

When entities like the Departments of Commerce and State, the United States Trade Representative, and the White House Office of Science and Technology Policy are relegated to the role of "advisors" to Team Telecom instead of being "members" and actively part of the risk assessment and deliberative process, there is a lack of representation from those agencies responsible for protecting economic national security interests. That is why we believe that the Department of Commerce's National Telecommunications and Information Administration should play a leading role in running the Team Telecom process.

3. ***Mr. Stehlin, what is the cause of this increased timeline, and how does this delay impact the planning and laying of subsea cables? Given the limited number of manufacturers that make these cables and the few ships available for laying and servicing cables, are there also supply chain implications?***

Response*:* As mentioned above, the duplicative nature of the Team Telecom process often leads to multiple rounds of back and forth between an applicant and any of the Team Telecom agencies. This delay dramatically increases the costs of a subsea cable system. On top of delaying a realization of increased capacity and redundancy, each day the application is delayed pushes the return on investment period further into the future, while also introducing risks related to availability of ships, suppliers, weather, terrain, and permitting. Additionally, any purchased materials begin to depreciate and plan modification may be needed in order to successfully deploy the cable.

The Honorable Doris Matsui

1. ***Open RAN increases supply chain diversity – which has significant economic, network performance, and national security benefits.***

Mr. Stehlin, how can Open RAN and secure-by-design principles help our networks be more trusted and resilient?

Response: Open RAN and secure-by-design principles play a vital role by supporting supply chain diversity, increasing resilience, and encouraging innovation in the trusted nations' tech ecosystem. Although these principles raised in this question are possibly related, they are two distinct items. Open RAN's interoperable architecture potentially reduces dependency on foreign adversary controlled equipment manufacturers by creating a marketplace for interchangeable equipment made by trusted manufacturers. From a resilience standpoint, Open RAN potentially improves the ability of operators to integrate components from multiple suppliers, avoiding single points of failure and enabling quicker recovery from disruptions, assuming that the systems integration is successful. But like any network architecture, Open RAN solutions must be proven from a security perspective and need to be shown to meet secure-by-design principles.

The secure-by-design approach reinforces resiliency by ensuring that systems are built with layered defenses, limited attack surfaces, zero-trust, and robust monitoring from the outset. TIA strongly believes that security must be built into our networks, which is why we created SCS 9001, our supply chain security standard, to allow ICT industry to certify that their products and networks are built with a defense-in-depth approach to network technology. We feel SCS, and similar secure-by-design principles create a foundation for agile, trusted, and future-ready networks that are better equipped to serve national interests and protect against emerging threats. Security starts with the processes an organization uses to build a product or service.

2. ***California is a major landing site for undersea cables, which connect us to the rest of the world and are a part of a global system carrying 99 percent of international data traffic.***

Telecommunications Industry Association
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209 | www.tiaonline.org

Mr. Stehlin, what role does redundancy play in both preventing and mitigating the effects of deliberate or accidental disruptions to our subsea cable networks?
Mr. Stehlin, your testimony indicates that regulatory delays have reduced cable redundancy. Could you explain how these constraints increase national vulnerability and what reforms might help improve resilience?

Response: As in any communications system, redundancy plays a critical role in both preventing service outages and mitigating the effects of disruptions. Subsea cables form the backbone of global internet connectivity. If one cable is damaged or cut, subsea cable redundancy enables traffic to be automatically rerouted with minimal downtime. By spreading traffic across a diverse set of cable routes, physical geographies, and landing points, networks become more resilient to localized incidents or targeted attacks. As capacity demands on cables increase due to an uptick in the use of advanced digital technologies, it is critical to have redundant cables to avoid bottlenecks and slowdowns and to quickly and efficiently reroute traffic destined for diverse global endpoints.

As industry is rushing to increase the redundancy of our subsea cable infrastructure, regulatory uncertainty and delays slow down and raise the cost of deployment. When the PEACE subsea cable system crossing through the Red Sea was cut it took approximately three weeks to get the cable back online. Even if the Federal Communications Commission ("FCC") were to grant an emergency license to deploy a subsea cable system, it would be too late for the system to act as a backup. We need to work quickly to deploy cables now, so we can increase our cable route diversity and minimize disruptions to essential global communications and data flows. This can be done with an expedited Team Telecom review for trusted vendors; increased cooperation and information sharing between Team Telecom, the FCC, and trusted providers; and standardized mitigation and security measures, providing much needed regulatory certainty.

The Honorable Robin Kelly

1. ***Mr. Stehlin, many of our global communications travel across subsea cables. To protect these cables and the data, we need to address both the physical security and the cybersecurity of these cables. Regarding cybersecurity, how do you suggest we protect the actual data traveling across these cables?***

Response: The Federal government has a variety of cybersecurity requirements across all sectors of industry. In developing cybersecurity requirements in this area, it is important to recognize that the responsibility of subsea cable operators should be limited to ensuring the resiliency of the physical infrastructure they operate. Ensuring the confidentiality and integrity of data in transit across the Internet is typically the responsibility of the data's ultimate owner and the communications service provider, which can be a different entity than the subsea cable owner. Ensuring the infrastructure owner does not have access to data flowing over the cables is critical for privacy and civil liberties purposes, and the majority of traffic flowing over cables is protected by end-to-end encryption. Additionally, each network element in the subsea cable system should be purchased from trusted suppliers.

In many cases, communications providers must already develop cybersecurity plans that align to the National Institute of Standards and Technology ("NIST") Cybersecurity Framework under other appropriate and complementary regulatory regimes. Adopting a cybersecurity plan that adheres to the NIST Framework ensures that service providers have the flexibility and agility necessary to respond to a highly dynamic cyber threat environment.